6th Asian Academic Society International Conferenc (AASIC)
A Transformative Community:
Asia in Dynamism, Innovation, and Globalization

SMARTPHONE USING RISK BEHAVIORS FOR CYBERCRIME VICTIMISATION : A CASE STUDY OF KASETSART UNIVERSITY, BANG KHEN CAMPUS, STUDENTS

Pol.Cpl.Chetsadaphong Khamchu, Pol.Lt.Col.Seksan Khruakham, Ph.D.
Social Sciences Faculty, Royal Police Cadet Academy, Thailand
email: chetsadaphong.d@gmail.com

ABSTRACT

In 2001, mobile phone users were only 20% of the world's population, but the number of mobile phone users has dramatically increased to almost 100% of the world's population in 2017. The rapid change of technology has also brought the rapid change in lifestyles of people. For instance, smartphones have become one of the most useful devices in modern society. However, using a smartphone can be vulnerable to higher technology-crime victimization. Therefore, it is interesting to study smartphone using risk behaviors of being a cybercrime victim. This quantitative research was conducted by collecting data from the samples of 400 Kasetsart University, Bang Khen Campus, students selected by using stratified sampling method. The data were collected through online questionnaires and analyzed by using descriptive statistics including frequency, percentage, mean, and standard deviation and referential statistics including t-test and F-test. The results show that place of birth of smartphone users caused a significant difference in risk behaviors for cybercrime victimization at the significant level of 0.05, meanwhile, gender, age, faculty, and residence did not cause any significant difference in risk behaviors. In addition, it was found that the number of smartphones, number of phone number in service, smartphone using duration, smartphone using duration for social media, and smartphone operation system caused some significant differences in risk behaviors for cybercrime victimization. There were 3 risk behaviors in a rather high level for being a victim of cybercrime including (1) careless smartphone using that makes it easy to be stolen, (2) setting up auto - log in for many applications, and (3) using public wi-fi to get an access to the internet. However, most of the risk behaviors for cybercrime victimization of the sampled smartphone users were found at a rather low level.

Keywords: victimization, risk behaviors, cybercrime, smartphone, criminology

1. INTRODUCTION

In 2001, (International Telecommunication Union 2017) mobile phone users were only 20% of the world's population, but the number of mobile phone users has dramatically increased to almost 100% of the world's population in 2017, and more than 75% of them were connected to the internet via smartphone both 3G and LTE. Meanwhile, (World Bank 2018) number of internet users in Thailand were approximately a half of the country's population. The report of Global Risk Report 2018 (World Economic Forum 2018) showed that cybercrime threats were in the top five of risk circumstances. One of the risks from cyberspace, which the world will face, is a cyber attack, where more damages will be caused by using higher technology to attack the target's operation system such as WannaCry malware, disrupting infarstructure across the world including telecommunication provider, railway, banks, hospitals etc. Data theft and fraud is another risk that can occur to any individuals, who posted their indentification information on websites. As result, smartphones have become one of the most useful devices in modern society. However, using smartphone can be vulnerable to higher technology-crime victimization. Therefore, it is interesting to study smartphone using risk behaviors of being a cybercrime victim.

2. REVIEW OF RELATE LITERATURE

Three theoretical concepts were used to establish the conceptual framework in this study, including victim precipitation, the lifestyle-exposure theory and routine activity theory (Khruakham 2015). First, the victim precipitation approach by Marvin Wolfgang explains that crime victims often brought themselves to crime circumstances. In Amir's study, it was found that the victims in the studied rape cases also played a certain role in the cases. Second, the lifestyle-exposure theory explains the interaction between victims and their environmental and social circumstances. People who live in a vulnerable and risky location tend to be a criminal victim including cybercrime (Choi 2008). Lastly, routine activity theory explains crime is equal to "CRIME = (Offender + Target - Guardian) (Place + Time)", which means crime will occur when the motivated offender finds a suitable target, who lacks the capable guardian in a perfect place and in the right time (Andresen and Farrell 2014).

Smartphone risk and safety using behaviors can be found in the official websites of the involved organizations such as Thai-CERT. This research used the Thai-CERT smartphone safety usage principles as a guideline (Thai-CERT 2011). There are four types of cyber-threats to be concerned including: (1) Application-Based Threats, which were concerned with Malware, Spyware and Zero-day explosion, (2) Web-Base Threats, which were concerned with phishing website and cyber frauds, (3) Network Threats, which concerned with threats from Bluetooth, Wi-Fi and other connections on smartphone interfaces, and (4) Physical Threats, which were concerned with threats from smartphone losing.

3. RESEARCH METHOD

This quantitative research collected data from 400 samples who were selected by using a proportional stratified sampling method from the population of 26,589 bachelor's degree students in Kasetsart University, Bang Khen Campus Data were collected by employing online questionnaires, divided into 3 parts including: (1) Individual characteristics (gender, age, faculty, place of birth and resident), (2) Smartphone using characteristics (number of smartphones, number of phone number in service, smartphone using duration, smartphone using duration for social media, for leisure activities, for online banking, for education activities, kind of internet connection and smartphone operation system), and (3) Risk behaviors to be cybercrime victimization, containing 19 questions based on risk and safety behaviors to be cybercrime victimization. Online questionnaires could be accessed via the created QR code. The collected data were analyzed by using descriptive statistics including frequency, percentage, mean, and standard deviation and referential statistics including t-test and F-test at the significant level of 0.05 to test the hypotheses as follows:

H1: Individual characteristics have a relationship with risk behaviors for cybercrime victimization.

H2: Smartphone using characteristics have a relationship with risk behaviors for cybercrime victimization.

4. FINDING AND DISCUSSIONS

a. Risk behaviors for cybercrime victimization

Table 1: Risk behaviors for cybercrime victimization

Risk behaviors for cybercrime victimization	□	S.D.	Risk level
1. Careless smartphone using that makes it easy to be stolen.	4.12	1.47	rather high
2. Individual information was posted on social media services or many sources that are easy to be found.	2.53	1.33	rather low
3. Opening Bluetooth or Wi-Fi interface, although unknot in use.	3.20	1.52	rather low
4. Using public wi-fi to get an access to the internet.	3.68	1.29	rather high
5. Using to root or jailed break smartphone.	1.84	1.27	low
6. Telling password to other persons or other ways that allow others to know it.	2.75	1.31	rather low

Risk behaviors for cybercrime victimization	□	S.D.	Risk level
*7. Wiping out all data, when finishing using smartphone or changed it.	2.89	1.60	rather low
*8. Setting up a two-step authentication process for social media services or online banking.	2.70	1.43	rather low
*9. Backing up all data to cloud services or secured	3.08	1.32	rather low

offline sources.

*10. Reading important information before installing an application.	3.23	1.14	rather low
*11. Noticed that browsing internet by using secure protocol like https://	2.74	1.14	rather low
*12. Always updating operation system and application.	2.43	1.03	rather low
13. Using online banking services by connecting to Public Wi-Fi.	2.73	1.49	rather low
*14. Always setting up and activating lock screen.	1.71	1.03	Low
15. Saving username and password in smartphone memo application.	3.18	1.68	rather low
*16. When cyber threat has been found, taking action to reduce the impact of cybercrime threat like changing password.	2.62	1.31	rather low
*17. Considering an authorization of application to access to data sources in smartphone.	2.71	1.18	rather low
*18. Setting up a complicated password, 6 – 8 alphabets including capital and normal alphabets, numbers and symbols.	2.16	1.05	low
19. Setting up auto - log in for many applications	3.79	1.38	rather high
Total	**2.85**	**0.48**	**rather low**

* sign is referred to positive questionnaires (safety smartphone using behaviors), by the way data analysis was transferred to negative questionnaires (risk smartphone using behaviors).

Research findings show that the samples had a rather low level for being a victim of cybercrime (□=2.85, S.D.=0.48). This could be explained that the samples were not likely to be suitable targets for cybercrime because they had enough knowledge to use their smartphones safely, according to routine activity theory. However, three risk behaviors were found to be at a rather high level, including careless smartphone using that makes it easy to be stolen (□=4.12, S.D.=1.47), setting up auto - log in for many applications (□=3.79, S.D.=1.38) and using public wi-fi to get an access to the internet (□=3.69, S.D.=1.29).

b. Hypothesis testing

1. Individual Characteristic

The results show that place of birth of smartphone users caused a significant difference in risk behaviors for cybercrime victimization at the significant level of 0.05, meanwhile, gender, age, faculty, and residence did not cause any significant difference in risk behaviors. The results of hypothesis testing showed that an Individual characteristic, place of birth of smartphone users caused a significant difference to risk behaviors for cybercrime victimization at the significant level of 0.05 as shown in table 2.

Table 2: A comparison of risk behaviors for cybercrime victimization by place of birth

	Place of birth	n	□	S.D.	t	Sig.
Risk behaviors	Bangkok and nearby	231	2.89	0.49	2.27	0.02

County side	169	2.78	0.46

The result of a comparison of risk behaviors for cybercrime victimization by place of birth using a t-test analysis showed a significant difference at the significant level of 0.05 (t=2.27, Sig.=0.02). This means that the samples who had the place of birth in Bangkok and nearby had a higher level of risk behaviors for cybercrime victimization than the samples who had the place of birth in county side. This is because the samples that lived in Bangkok can get accessed to the internet more frequently than the samples that lived outside Bangkok.

2. Smartphone using characteristic

Regarding the smartphone using characteristics, it was found that the number of smartphones, the number of phone number in service, smartphone using duration, smartphone using duration for social media, and the smartphone operation system caused some significant differences to risk behaviors for cybercrime victimization.

Table 3: Comparison between number of smartphones using by samples and risk behaviors for cybercrime victimization

Number of smartphones		Use a smartphone	Use 1 - 2 smartphones	Use more than 2 smartphones
	□	2.83	3.02	2.32
Use one smartphone	2.83	-	-0.19*	0.52
Use 1 - 2 smartphones	3.02		-	0.70*
Use more than 2 smartphones	2.32			-

* significant at 0.05

The result in table 3 showed that the samples who use one smartphone had a significant level of difference of risk behaviors for cybercrime victimization. To be more specific, with the samples who use 1 – 2 smartphones (□=3.02) had a significantly higher level of risk behaviors for cybercrime victimization than the sample who use one smartphone (□=2.83) and who used more than 2 smartphones (□=2.32). This finding should be explained by the lifestyle-exposed theory in which the samples who used more smartphones should be likely to become a cybercrime victim.

Table 4: Comparison between number of phone number in service and risk behaviors for cybercrime victimization

Number of phone number in service	$\bar{X}$	A phone number	1 - 2 phone numbers	More than 2 phone numbers
	□	2.86	2.86	2.86
One phone number	2.86	-	0.12	1.05*
1 - 2 phone numbers	2.75		-	0.93*
More than 2 phone numbers	1.82			-

* significant at 0.05

The result in table 4 showed that samples who use more than 2 phone numbers had significant differential level of risk behaviors for cybercrime victimization. To be more specific, with the samples who used one phone number (□=2.86) had a significantly higher level of risk behaviors for cybercrime victimization than the samples who use 1 - 2 phone numbers (□=2.75) and samples who use more than 2 phone numbers (□=1.82). This finding should be explained by the lifestyle-exposed theory in which the samples who used more phone numbers should be likely to become a cybercrime victim.

Table 5: Comparison between smartphone using duration and risk behaviors for cybercrime victimization

Smartphone using duration		0 – 6 months	6 - 12 months	More than 12 months
	□	2.97	2.77	2.83
0 – 6 months	2.97	-	0.20*	0.14*
6 - 12 months	2.77		-	-0.07
More than 12 months	2.83			-

* significant at 0.05

The result in table 5 showed that samples who used their smartphones 0 – 6 months had significant differential level of risk behaviors for cybercrime victimization. To be more specific, with the samples who use their smartphones 0 – 6 months (□=2.97) had a significantly higher level of risk behaviors for cybercrime victimization than the samples who use smartphone more than 12 months (□=2.83) and samples who use their smartphones 6 – 12 months (□=2.77). This finding should be explained by the lifestyle-exposed theory in which the samples who had the longest duration of smartphone using should be likely to become a cybercrime victim.

Table 6: Comparison between smartphone using duration for social media and risk behaviors for cybercrime victimization

smartphone using duration for social media		1 - 2 hrs. a day	2 - 4 hrs. a day	More than 4 hrs. a day
	$\bar{X}$	2.6608	2.8703	2.8767
1 - 2 hrs. a day	2.6608	-	-0.21*	-0.22*
2 - 4 hrs. a day	2.8703		-	-0.01
More than 4 hrs. a day	2.8767			-

* significant at 0.05

The result in table 6 showed that samples who use their smartphones for social media 1 - 2 hrs. a day had significant differential level of risk behaviors for cybercrime victimization. To be more specific, with the samples who use smartphones for social media more than 4 hrs. a day (□=2.8767) had a significantly higher level of risk behaviors for cybercrime victimization than the samples who use their smartphones for social media 2 - 4 hrs. a day (□=2.8703) and samples who use their smartphones for social media 1 - 2 hrs. a day (□=2.6608). significantly. This finding can be explained by the lifestyle-exposed theory. For instance, Kyung-Shick Choi's (2008) study found that the more levels of online vocational activities and leisure activities which interacted with cyberspace brought the risk-taking factors to be cybercrime victim.

Table 7: A comparison of risk behaviors for cybercrime victimization by smartphone operation system

	Smartphone Operation System	n	□	S.D.	t	Sig.
Risk behaviors	IOS	264	2.89	0.47	2.35	0.02
	Android	136	2.77	0.50		

The result of a comparison of risk behaviors for cybercrime victimization by smartphone operation system using a t-test analysis showed a significant difference at the significant level of 0.05 (t=2.35, Sig.=0.02). This means that the samples who used IOS had a higher level of risk behaviors for cybercrime victimization than the samples who used Android. This is because the samples that used IOS can get accessed to the internet more frequently than the samples that used Android.

5. RECCOMMENDATIONS AND CONCLUSIONS

Based on the findings in this study, some recommendations are worth discussing as following:

(1) Since three risk behaviors of smartphone users were found to be rather high, including: careless smartphone using that makes it easy to be stolen, using public wi-fi to get an access to the internet and setting up auto - log in for many applications, it is suggested that)1) people should take care of their smartphones, by not leaving their phones away from their sight, (2) people should be noticed that public wi-fi is harmful and should be avoided, if it is necessary to use a public wi-fi, they should make sure that they connect to the reliable one and (3) people should avoid setting up an auto login, in particular for financial applications.

(2) Law enforcement organizations getting involved in cyber-security and cyber-investigation should create a program to increase public awareness of cybercrime prevention for people, who especially live in Bangkok or urban areas, have more than one smartphone, and use it for social media to decrease the level of risk behaviors for cybercrime victimization.

(3) The smartphone operation system can help users to be safer when surfing the internet. Therefore, people should choose a smartphone based on the operation system.

6. REFERENCES

Online Reports: International Telecommunication Union. (2017). “Measuring the Information Society Report Volume 1.” (online), URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1. pdf.

Online Journals: Kyung-Shick Choi. (2008). “Computer Crime Victimization and Integrated Theory: An Empirical Assessment.” URL: http://www.cybercrimejournal.com/Choiijccjan2008.htm. International Journal of Cyber Criminology, January-June 2008, Vol 2 (1), 308–333.

eBook: Marilyn McShane. (2013). “An Introduction to Criminological Theory.” Taylor & Francis Group. eBook ISBN: 9781135632663.

eBook: Martin A. A., and Graham F. (2015). “Criminal Act: The Role and Influence of Routine Activity Theory.” Palgrave Macmillan Limited. eBook ISBN: 9781137391322.

Book: Seksan Khruakham. (2015). “Criminology and Criminal Justice.” Nakhonprathom. Thailand.

Online: Thai-CERT. (2011). “Smartphone safety using principle from cyber-threat.” (online), URL: https://www.thai cert.or.th /papers/general/2011/pa2011ge010.html.

Online: World Bank. (2018). “Individuals using the Internet (% of population).” (online), URL:https://data.worldbank.org /indicator/IT.NET.USER.ZS.

Online Reports: World Economic Forum. (2018). “The Global Risks Report 2018, 13th Edition.” (online), URL: http:// reports.weforum.org/global-risks-2018.